REMARKS/ARGUMENTS

Favorable reconsideration of this application as presently amended and in light of the following remarks is respectfully requested.

Claims 1-3 and 6-26 are pending in the present application. Claims 1, 11, 13, 15-18, 21, 22, 25 and 26 are amended by the present amendment.

Applicants respectfully submit that claim amendments find support in the specification as originally filed. Thus, no new matter is added.

In the outstanding Official Action, Claims 1-9 and 11-18 were rejected under 35 U.S.C. § 102(e) as anticipated by European Patent Application EP 0982895 to Shimizu et al. (herein "Shimizu"); and Claim 10 was rejected under 35 U.S.C. § 103(a) as unpatentable over Shimizu in view of U.S. Patent No. 5,933,501 to Leppek. Applicants respectfully traverse the rejections with respect to the amended independent claims.

Amended Claim 1 is directed to an apparatus based on a common key encryption system in which a plurality of expanded keys are used in a predetermined order. The apparatus includes, in part, a plurality of round processing circuits that comprise a first portion including at least two round processing circuits having first and second round functions and a second portion which follows the first portion. The second portion includes at least two round processing circuits having third and fourth round functions, the third round function being an inverse of the second round function, and the fourth round function being an inverse of the first round function. Independent Claims 11, 13 and 15-18 include similar features.

In a non-limiting example, Applicants' Figure 1 shows an apparatus that includes an expanded key scheduling section 3 having a plurality of round processing circuits 31_1 to 31_n. Though an involution function is a function that is its own inverse, the expanded key scheduling section 3 comprises at least a first round function and a second round function

12

which is an inverse function of the first round function. Stated another way, the present invention relates to round functions which are mutually inverse.

Applicants' respectfully submit that Shimizu does not teach or suggest a plurality of round processing circuits that comprise at least two round processing circuits having mutually inverse round functions. Shimizu merely indicates that "there is no limitation on a function to be employed in the key conversion section with the exception that an original key is converted by using an involution function."[1] However, Shimizu does not indicate any mutually inverse round functions. Accordingly, Applicants' respectfully submit that Shimizu does not teach or suggest "at least two round processing circuits having third and fourth round functions, the third round function being an inverse of the second round function, and the fourth round function being an inverse of the first round function," as recited in independent Claim 1, and as similarly recited in independent Claims 11, 13 and 15-18.

Further, Applicants respectfully submit that Shimizu also does not teach or suggest that a sub key output from a round processing circuit of a last state is a common key.

Shimizu merely indicates that "it is not necessary for an encryption key and a decryption key to be same."[2] Shimizu does not indicate that the encryption key and the decryption key must be the same. In order to make the encryption key equal to the decryption key, it is necessary to impose a limitation on the round functions included in the expanded key scheduling section. Further, the present invention aims to use the same round processing circuits or the same portion of the round processing circuits of the expanded key scheduling section for an encryption circuit and the expanded key scheduling section for a decryption circuit.

In order to satisfy both the requirements, the expanded key scheduling section can employ the round processing configuration, such as shown in the non-limiting example of

---

[1] Shimizu at column 3, lines 28-31(emphasis added).
[2] Shimizu at column 3, lines 32-33.

Applicants' Figures 3, 5, 7, 8, and 9. As Applicants further describe in the specification at page 26, line 21 to page 29, line 16, if the round processing configuration is employed, a series of round functions in the encryption apparatus is identical to a series of round functions in the decryption apparatus. For example, if the round functions of eight stages in the decryption apparatus are f_1, f_2, f_3, f_4, f_4^{-1}, f_3^{-1}, f_2^{-1}, and f_1^{-1}, the round functions of eight stages in the decryption apparatus becomes inverse functions of these functions, i.e., $(f_1^{-1})^{-1}$, $(f_2^{-1})^{-1}$, $(f_3^{-1})^{-1}$, $(f_41)^{-1}$, $(f_4)^{-1}$, $(f_3)^{-1}$, $(f_2)^{-1}$, and $(f_1)^{-1}$. Therefore, the result is f_1, f_2, f_3, f_4, f_4^{-1}, f_3^{-1}, f_2^{-1}, and f_1^{-1}, and it is found that both of them coincide with each other. This means that the same round processing circuits can be used for both the encryption apparatus and the decryption apparatus.

Further, it is not necessary to employ the round trip configuration for all of the round processing circuits. As shown in Applicants' non-limiting example of Figures 7, 8, and 9, it is possible to employ the round trip configuration for a part of the round processing circuits. The expanded key scheduling section of the present invention may include at least the following limitation:

(input), *, ..., *, fa, fb, *, ..., *, (fb^{-1}), (fa $^{-1}$), *,..., *, (output)

where * indicates any function.

The teaching of <u>Shimizu</u> differs from the present invention since <u>Shimizu</u> aims to enable generation of an extended key in a reverse order by using the involution function in a reverse order based on a decryption key in decryption, and uses a key which is a result of processing an encryption key in a key conversion section.[3] Thus, as shown by FIGS. 2 and 3 of <u>Shimizu</u>, the key transformation section 2 in the encryption device generates the key by using the round functions fk-1, fk2, ..., fkn and the key transformation section 2 in the decryption device generates the key by using the round functions fkn, fkn-1, ..., fk1.

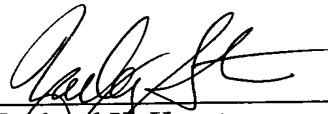[3] <u>Shimizu</u> at paragraph [0019].

Therefore, according to <u>Shimizu</u> it is not possible to use the same key conversion section for both the encryption device and the decryption device.

Accordingly, it is respectfully submitted that <u>Shimizu</u> clearly does not anticipate or render obvious the claimed subject matter, and further, that the deficiencies of <u>Shimizu</u> are not remedied by <u>Leppek</u>. It is therefore respectfully submitted that the outstanding grounds for rejection on the merits have been overcome.

Consequently, in view of the present amendment and in light of the above discussion, no further issues are believed to be outstanding, and the present application is believed to be in condition for formal allowance. An early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Eckhard H. Kuesters
Attorney of Record
Registration No. 28,870

Zachary S. Stern
Registration No. 54,719

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 06/04)

EHK:ZSS:dnf

I:\ATTY\ZS\21's\211\211428US\211428 AMD 022406.DOC

15